UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,511	12/20/2000	Peter Landrock	105005-0044C1	3110

24267 7590 05/18/2004

CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

EXAMINER	
YOUNG, JOHN L	

ART UNIT	PAPER NUMBER
3622	

DATE MAILED: 05/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/747,511	LANDROCK, PETER
	Examiner	Art Unit
	John L Young	3622

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

JOHN LEONARD YOUNG, ESQ.
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

NON-FINAL REJECTION

DRAWINGS

1. This application has been filed with drawings that are considered informal; said drawings are acceptable for examination purposes. The review process for drawings that are included with applications on filing has been modified in view of the new requirement to publish applications at eighteen months after the filing date of applications, or any priority date claimed under 35 U.S.C. §§119, 120, 121, or 365.

CLAIM AMENDMENT OBJECTION — 37 CFR §1.121

2. **Objection Withdrawn.**

CLAIM REJECTIONS — 35 U.S.C. §101

35 U.S.C. §101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

3. Claims 25-32 & 36-61 are rejected under 35 U.S.C. 101, because said claim is directed to non-statutory subject matter.

As per claim 25, as drafted said claim is not limited by language within the technological arts (see *In re Waldbaum*, 173 USPQ 430 (CCPA 1972); *In re Musgrave*, 167 USPQ 280 (CCPA 1970) and *In re Johnston*,

183 USPQ 172 (CCPA 1974) also see MPEP 2106 IV 2(b) albeit limited to a useful, concrete and tangible application (See *State Street v. Signature financial Group*, 149 F.3d at 1374-75 , 47 USPQ 2d at 1602 (Fed Cir. 1998) ; *AT&T Corp. v. Excel*, 50 USPQ 2d 1447, 1452 (Fed. Cir. 1999). Note: it is well settled in the law that "[although] a claim should be interpreted in light of the specification disclosure, it is generally considered improper to read limitations contained in the specification into the claims. See *In re Prater*, 415, F.2d 1393, 162 USPQ 541 (CCPA 1969) and *In re Winkhaus*, 527 F.2d 637, 188 USPQ 129 (CCPA 1975), which discuss the premise that one cannot rely on the specification to impart limitations to the claims that are not recited in the claims." (See MPEP 2173.05(q)).

In this case, the claim language is merely non-functional descriptive material disembodied from the technological arts.

Claims 26-32 and 36-61 are rejected for substantially the same reason as claim 25.

CLAIM REJECTIONS — 35 U.S.C. §103(a)

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Independent claims 25 & 36 and dependent claims 26, 27, 30, 31, 34, 35, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56 & 58 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen 5,557,518 (09/17/96) [f/d: 4/28/94] (herein referred to as "Rosen") in view of Chang 5,724,425 (3/3/1998) [US f/d: 6/10/1994] (herein referred to as "Chang").

As per claim 25, Rosen (col. 23, ll. 9-51) shows elements that suggest a "method of issuing an electronic negotiable document. . . ." [i.e., *"electronic money"*].

Rosen (col. 16, ll. 19-20) shows elements that suggest "a unique public-secret key pair for signing and verifying. . . ."

Rosen (col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; and FIG. 1 and FIG. 2) shows elements that suggest "creating as data an END and storing this in a tamper-resistant document carrier, the document carrier containing a . . . verifying and a unique document carrier identifier . . . and storing the result in the document carrier."

Rosen does not explicitly show "signing the unique document-carrier identifier. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "signing the unique document-carrier identifier. . . ." because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12). Furthermore,

Rosen does not explicitly show a tamper-resistant document carrier.

Chang (col. 1, ll. 35-50) discloses: "Public key systems may also be used to encrypt messages, and also to effectively sign messages. . . . [and] to seal or render tamper-proof a piece of data. . . . The sender packages the data, the message digest and the public key together. The receiver may check for tampering by computing the message digest again, then decrypting the received message digest with the public key." The Examiner interprets this disclosure as showing a tamper-resistant document carrier.

Chang proposes tamper-resistant document carrier modifications that would have applied to the system of Rosen. It would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the disclosure of Chang with the teachings of Rosen because such combination would have provided means of *"utilizing public key encryption techniques for enhancing software security and for distributing software."*

As per claim 26, Rosen in view of Chang shows the method according to claim 25 above.

Rosen (FIG. 2, els. 42, 56, 68, 82, 92, 98, 106, 112, and 116) shows elements that suggest "generating a time stamp representing the time of issue. . . ."

Rosen does not explicitly show "storing this . . . [time stamp] with the END in the tamper-resistant document carrier before the encryption step. "

Rosen (col. 6, ll. 37-43) shows *'Time Purchased field . . . a Decryption Keys field . . . for decrypting if the communication is encrypted. . . ."*

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen *"Time Purchased field . . . a Decryption Keys field . . . for decrypting if the communication is encrypted. . . ."* would have been selected in accordance with "storing this . . . [time stamp] with the END in the tamper-resistant document carrier before the encryption step. . . ." because such time stamp storing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 27, Rosen in view of Chang shows the method according to claim 25 above.

Rosen (col. 12, ll. 6-8) shows elements that suggest "calculating a hash value of the end and/or the time stamp value and storing this hash value instead of the full end in the tamper-resistant document carrier. . . ."

Rosen does not explicitly show "storing this . . . [hash function] . . . before the encryption step. "

Rosen (col. 6, ll. 37-43) shows *"a Decryption Keys field . . . for decrypting if the communication is encrypted. . . ."*

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's *"Decryption Keys field . . . for decrypting if the communication is encrypted. . . ."* would have been selected in accordance with "storing this . . . [hash function] . . . before the encryption step. . . ." because such hash function storing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 30, Rosen in view of Chang shows the method according to claim 25 above.

Rosen (col. 11, ll. 62-67; and col. 12, ll. 6-15) shows elements that suggest "calculating a hash value of the data to be encrypted by said secret key, in place of the full data."

Rosen does not explicitly show "calculating a hash value of the data to be encrypted by said secret key, in place of the full data."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's *"certificate validation protocols . . .* [which include] *hash . . . and encrypting . . . applications. . . ."* would have been selected in accordance with "calculating a hash value of the data to be encrypted by said secret key, in place of the full data. . . ." because such applications would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 31, Rosen in view of Chang shows the method according to claim 25 above.

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "the document carrier stores a negotiability status flag indicative of whether the END stored therein in negotiable or non-negotiable, and including the step of setting the flag to 'negotiable' after the result of the encryption has been stored in the document carrier."

Rosen does not explicitly show "the document carrier stores a negotiability status flag indicative of whether the END stored therein in negotiable or non-negotiable,

and including the step of setting the flag to 'negotiable' after the result of the encryption has been stored in the document carrier."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's *"a Status field . . . indicating whether the ticket is unused or has already been used. . . ."* would have been selected in accordance with "the document carrier stores a negotiability status flag indicative of whether the END stored therein in negotiable or non-negotiable, and including the step of setting the flag to 'negotiable' after the result of the encryption has been stored in the document carrier. . . ." because such status indication would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Dependent claim 33 is rejected for substantially the same reasons as claim 25.

Dependent claim 34 is rejected for substantially the same reasons as claim 31.

Dependent claim 35 is rejected for substantially the same reasons as claim 32.

As per claim 36, Rosen (col. 23, ll. 9-51; and FIG. 1) shows elements that suggest a "method of negotiating an END [i.e., *"electronic money"*] between seller and a buyer each possessing a tamper-resistant document carrier. . . ."

Rosen (col. 16, ll. 19-20; col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; FIG. 1 and FIG. 2) shows elements that suggest a "carrier having

its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data. . . . sending the public encryption key of the buyer's document carrier to the seller's document carrier. . . . using . . . [the public encryption key] to encrypt the message comprising the END together with the negotiability status flag. . . ."

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers . . . [and] aborting the negotiation if not. . . ."

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the negotiability status flag, sending that encrypted message to the buyer, decrypting the message using the buyer's secret decryption key, and setting the negotiability status flag for the END of the buyer's and seller's document carriers respectively to **'negotiable and non-negotiable'**".

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "a negotiability status flag indicative of whether the END is currently negotiable from the document carrier on which it is stored. . . . [and] verifying in the seller's document carrier that the negotiability status flag is negotiable"

Rosen does not explicitly show "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ." because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Rosen does not explicitly show a tamper-resistant document carrier.

Chang (col. 1, ll. 35-50) discloses: "Public key systems may also be used to encrypt messages, and also to effectively sign messages. . . . [and] to seal or render tamper-proof a piece of data. . . . The sender packages the data, the message digest and the public key together. The receiver may check for tampering by computing the message digest again, then decrypting the received message digest with the public key." The Examiner interprets this disclosure as showing a tamper-resistant document carrier.

Chang proposes tamper-resistant document carrier modifications that would have applied to the system of Rosen. It would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the disclosure of Chang with the teachings of Rosen because such combination would have provided means of *"utilizing public key encryption techniques for enhancing software security and for distributing software."*

As per claim 38, Rosen in view of Chang shows the method according to claim 36.

Rosen (col. 15, ll. 15-67; col. 16, ll. 19-67; col. 17, ll. 1-40; and col. 18, ll. 17-35) shows elements that suggest "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key."

Rosen does not explicitly show "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-35) *"[validate] issuer certificate and check issuer signature. . . . Verify . . . identifiers. . . . Validate each sender certificate and check each sender signature. Verify . . . receiver identifier. . . . "* would have been selected in accordance with "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key. . . ." because such credentials would have provided an *"electronic object integrity . . . check. . . . "* (See Rosen col. 6, ll. 11-12).

As per claim 40, Rosen in view of Chang shows the method according to claim 38.

Rosen (FIG. 2 and col. 16, ll. 27-37) shows elements that suggest "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier."

Rosen does not explicitly show "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 16, ll. 27-37) *"both . . . have stored the . . . session key . . . to be used for their current interaction in recertifying. . . ."* would have been selected in accordance with "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier. . . ." because such certification would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 42, Rosen in view of Chang shows the method according to claim 38.

Rosen (FIG. 2; FIG. 1; and col. 16, ll. 27-37) shows elements that suggest "the certificate of the buyer's document carrier is sent to the seller's document carrier. . . ."

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; col. 40, ll. 14-29; and col. 18, ll. 17-37) shows elements that suggest "the certificate of the buyer's document carrier . . . is authenticated and the negotiation is aborted if authentication fails."

Rosen does not explicitly show "the negotiation is aborted if authentication fails."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-37) *"[if] the . . . credential is not valid, then the transaction is aborted. . . ."* would have been selected in accordance with "the negotiation is aborted if authentication fails. . . ." because such validation would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 44, Rosen in view of Chang shows the method according to claim 36.

Rosen (col. 16, ll. 19-20) shows elements that suggest a "secret key, verifies the signature of the issuer on the END. . . ."

Rosen (FIG. 1; FIG. 2; FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; col. 40, ll. 14-29; and col. 18, ll. 17-37) shows elements that suggest "the buyer's document carrier after decrypting the message using its secret key, verifies the signature of the issuer on the END, and informs the issuer in the event that authentication fails."

Rosen does not explicitly show "after decrypting the message using its secret key, verifies the signature of the issuer on the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-35) *"[validate] issuer certificate and check issuer signature. . . . Verify . . . identifiers. . . . Validate each sender certificate and check each sender signature. Verify . . . receiver identifier. . . . "* would have been selected in accordance with "after decrypting the message using its secret key, verifies the signature of the issuer on the END. . . . . ." because such verification would have provided an *"electronic object integrity . . . check. . . . "* (See Rosen col. 6, ll. 11-12).

As per claim 46, Rosen in view of Chang shows the method according to claim 25.

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "issuing an END on a document-carrier. . . . [preceding] a method of negotiating an END. . . ."

Rosen (col. 23, ll. 9-51; and FIG. 1) shows elements that suggest a "method of negotiating an END [i.e., *"electronic money"*] between seller and a buyer each possessing a tamper-resistant document carrier. . . ."

Rosen (col. 16, ll. 19-20; col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; FIG. 1 and FIG. 2) shows elements that suggest a "carrier having its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data. . . . sending the public encryption key of the buyer's document carrier to the seller's document carrier. . . . using . . . [the public encryption key] to encrypt the message comprising the END together with the negotiability status flag. . . ."

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers . . . [and] aborting the negotiation if not. . . ."

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the negotiability status flag, sending that encrypted message to the buyer, decrypting the message using the buyer's secret decryption key, and setting the negotiability status flag for the END of the buyer's and seller's document carriers respectively to **'negotiable and non-negotiable'"**.

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "a negotiability status flag indicative of whether the END is currently negotiable from the document carrier on which it is stored. . . . [and] verifying in the seller's document carrier that the negotiability status flag is negotiable"

Rosen does not explicitly show "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the*

time it was signed. . . . "would have been selected in accordance with "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . ." because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Dependent claim 48 is rejected for substantially the same reasons as claim 36.

As per claim 50, Rosen in view of Chang shows the method according to claim 48.

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "the buyer's document carrier. . . ."

Rosen (col. 16, ll. 19-20) shows elements that suggest a "secret key, verifies that the END is still valid. . . ."

Rosen (col. 6, ll. 37-43) shows elements that suggest "after decrypting the message with its secret key . . . taking its time stamp. . . ."

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100; and FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that

suggest "if . . . [the time stamp] has expired, informs the issuer of this, and aborts the negotiation before **incrementing** the counter or setting the negotiation status flag."

Rosen does not explicitly show "if . . . [the time stamp] has expired, informs the issuer of this. . . ."; however, it would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "if . . . [the time stamp] has expired, informs the issuer of this, and aborts the negotiation before incrementing the counter or setting the negotiation status flag. . ." because such time stamp validation would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 52, Rosen in view of Chang shows the method according to claim 36.

Rosen (FIG. 2; FIGs. 30A-E; col. 15, ll. 15-65; col. 16, ll. 1-67; col. 7, ll. 29-41; and col. 41, ll. 37-39) shows elements that suggest "recovering the negotiation of an END which has previously broken down, by providing the buyer's document-carrier with the necessary secret key which has been reproduced by the issuer or by a trusted third party."

Rosen does not explicitly show "recovering the negotiation of an END. . . ."; however, it would have been obvious to one of ordinary skill in the art of secure transactions that Rosen (FIG. 2; FIGs. 30A-E; col. 15, ll. 15-65; and col. 16, ll. 1-67) *"recertifying A's certificate. . . ."* would have been selected in accordance with

"recovering the negotiation of an END. . . ." because such recertifying validation would have provided an *"electronic object integrity . . . check. . . ."*(See Rosen col. 6, ll. 11-12).

As per claim 54, Rosen in view of Chang shows the method according to claim 36.

Rosen (col. 41, ll. 37-39) shows elements that suggest "an END lost from a primary document-carrier. . . ."

Rosen (col. 13, ll. 5-15; col. 13, ll. 35-60; and col. 20, ll. 31-42) shows elements that suggest "recovering an END lost from a primary document-carrier, by activating a back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier."

Rosen does not explicitly show a "back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 20, ll. 38-42) *"[the] overall system security pertaining to the money modules may be integrated with that for the trusted agents . . . but is preferably separate to provide for enhanced system security and system flexibility. . . ."* would have been selected in accordance with a "back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier. . . ." because such back-up capability would have provided an *"electronic object integrity . . . check. . . ."*(See Rosen col. 6, ll. 11-12).

As per claim 56, Rosen in view of Chang shows the method according to claim 52.

Rosen (col. 15, ll. 3-37) shows elements that suggest "inhibiting the recovery until the expiry of the predetermined period of validity of the END."

Rosen does not explicitly show "expiry of the predetermined period of validity of the END."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 15, ll. 3-11) *"[if] the timer expires before the message has been received, then Session Manager A will query Session Manager B to determine if the transaction is still running in B. If B does not reply, then Session Manager will abort the transaction. . . . A similar time-out function exists in the money modules. . . ."* would have been selected in accordance with "expiry of the predetermined period of validity of the END. . . ." because such a validity transaction would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 58, Rosen in view of Chang shows the method according to claim 54.

Rosen (col. 15, ll. 3-37) shows elements that suggest "inhibiting the recovery until the expiry of the predetermined period of validity of the END."

Rosen does not explicitly show "expiry of the predetermined period of validity of the END."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 15, ll. 3-11) *"[if] the timer expires before the message has been received, then Session Manager A will query Session Manager B to determine if the transaction is still running in B. If B does not reply, then Session Manager will abort the transaction. . . . A similar time-out function exists in the money modules. . . ."* would have been selected in accordance with "expiry of the predetermined period of validity of the END. . . ." because such a validity transaction would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

5. Dependent claim 28 is rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen 5,557,518 (09/17/96) [f/d: 4/28/94] (herein referred to as "Rosen") in view of Chang and further in view of Pitroda 5,590,038 (12/31/96) [f/d: 6/20/94] (herein referred to as "Pitroda").

As per claim 28, Rosen in view of Chang shows the method according to claim 25 above.

Rosen does not explicitly show "the document carrier identifier is a device number, and the END identifier is a serial number."

Pitroda (col. 15, ll. 58-63; and col. 16, ll. 39-40) shows elements that suggest "the document carrier identifier is a device number, and the END identifier is a serial number." Pitroda proposes serial number and device number modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Pitroda to Rosen, because such modifications

would have provided a means of *"storing . . . various [types] of . . . numbers . . . [associated with] financial or personal transactional information."* (See Pitroda col. 2, ll. 55-61).

6. Dependent claim 29 is rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen in view of Chang and further in view Tel 5,354,097 (10/11/94) (herein referred to as "Tel").

As per claim 29, Rosen shows the method according to claim 25 above. (See the rejection of claim 25 supra).

Rosen does not explicitly show "the END identifier is supplemented with data representing a water mark unique to the issuer."

Tel (col. 1, ll. 22-26) discloses means to *"counteract forgery by providing a watermark. . . ."*

Tel proposes *"watermark"* modifications that would have applied to the systems and methods for secure transaction management of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Tel to Rosen, because implementation of such modifications would have provided a means of showing the authenticity of an original image.

7. Dependent claim 32 and independent claims 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57 & 59 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen in view of Chang and

further in view of Pitroda and further in view of Abraham 5,148,481 (09/15/92) (herein referred to as "Abraham").

As per claim 32, Rosen in view of Chang shows the method according to claim 25 above.

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100; FIG. 4A) shows elements that suggest "the times the END has been negotiated since issue. . . ."

Rosen does not explicitly show "the document carrier includes a counter for counting a serial number . . . setting the counter to zero after the result of the encryption has been stored in the document carrier."

Pitroda (col. 15, ll. 58-63; and col. 16, ll. 39-40) shows elements that suggest "the document carrier identifier is a device number, and the END identifier is a serial number." Pitroda proposes serial number modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Pitroda to Rosen, because such modifications would have provided a means of *"storing . . . various [types] of . . . numbers . . . [associated with] financial or personal transactional information."* (See Pitroda col. 2, ll. 55-61).

Abraham (col. 5, ll. 5-55; and FIG. 8) shows elements that suggest "the document carrier includes a counter for counting a serial number . . . setting the counter to zero after the result of the encryption has been stored in the document carrier."

Abraham proposes counter modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the

invention was made to a person having ordinary skill in the art to add the modifications taught by Abraham to Rosen, because implementation of such modifications would have provided a method of *"access control. . . . individually programmable by the application owner. . . ."*of a digital work. (See Abraham col. 1, ll. 60-65; and col. 2, ll. 1-5).

As per claim 37, Rosen (col. 23, ll. 9-51; and FIG. 1) shows elements that suggest a "method of negotiating an END [i.e., *"electronic money"*] between seller and a buyer each possessing a tamper-resistant document carrier. . . ."

Rosen (col. 16, ll. 19-20; col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; FIG. 1 and FIG. 2) shows elements that suggest a "carrier having its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data. . . . sending the public encryption key of the buyer's document carrier to the seller's document carrier. . . ."

Rosen does not explicitly show "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."*would have been selected in accordance with "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . ."

because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Rosen does not explicitly show "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda (col. 15, ll. 58-63; and col. 16, ll. 39-40) shows elements that suggest "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda proposes serial number modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Pitroda to Rosen, because such modifications would have provided a means of *"storing . . . various [types] of . . . numbers . . . [associated with] financial or personal transactional information."* (See Pitroda col. 2, ll. 55-61).

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers . . . [and] aborting the negotiation if it is not negotiable. . . ."

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "verifying in the seller's document carrier that the END, if it has been stored previously in that document carrier, has a different counter value this time and is therefore negotiable. . . ."

Rosen does not explicitly show a tamper-resistant document carrier.

Chang (col. 1, ll. 35-50) discloses: "Public key systems may also be used to encrypt messages, and also to effectively sign messages. . . . [and] to seal or render tamper-proof a piece of data. . . . The sender packages the data, the message digest and the public key together. The receiver may check for tampering by computing the message digest again, then decrypting the received message digest with the public key." The Examiner interprets this disclosure as showing a tamper-resistant document carrier.

Chang proposes tamper-resistant document carrier modifications that would have applied to the system of Rosen. It would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the disclosure of Chang with the teachings of Rosen because such combination would have provided means of *"utilizing public key encryption techniques for enhancing software security and for distributing software."*

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the counter, sending that encrypted message to the buyer. . . ."

Rosen does not explicitly show " using . . . [the public encryption key] to encrypt the message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham (col. 5, ll. 5-55; and FIG. 8) shows elements that suggest encrypting a "message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham proposes counter modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Abraham to Rosen, because implementation of such modifications would have provided a method of *"access control. . . . individually programmable by the application owner. . . ."* of a digital work. (See Abraham col. 1, ll. 60-65; and col. 2, ll. 1-5).

As per claim 39, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 37.

Rosen (col. 15, ll. 15-67; col. 16, ll. 19-67; col. 17, ll. 1-40; and col. 18, ll. 17-35) shows elements that suggest "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key."

Rosen does not explicitly show "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-35) *"[validate] issuer certificate and check issuer signature. . . . Verify . . . identifiers. . . . Validate each sender certificate and check each sender signature. Verify . . . receiver identifier. . . . "* would have been selected in accordance with "each document carrier is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key. . ." because such credentials would have provided an *"electronic object integrity . . . check. . . . "* (See Rosen col. 6, ll. 11-12).

As per claim 41, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 39.

Rosen (FIG. 2 and col. 16, ll. 27-37) shows elements that suggest "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier."

Rosen does not explicitly show "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 16, ll. 27-37) *"both . . . have stored the . . . session key . . . to be used for their current interaction in recertifying. . . . "* would have been selected in accordance with "the certificate unique to the document carrier on which the END was originally issued is stored with the END in the seller's document carrier. . . ." because

such certification would have provided an *"electronic object integrity . . . check. . . ."*(See Rosen col. 6, ll. 11-12).

As per claim 43, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 39.

Rosen (FIG. 2; FIG. 1; and col. 16, ll. 27-37) shows elements that suggest "the certificate of the buyer's document carrier is sent to the seller's document carrier. . . ."

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; col. 40, ll. 14-29; and col. 18, ll. 17-37) shows elements that suggest "the certificate of the buyer's document carrier . . . is authenticated and the negotiation is aborted if authentication fails."

Rosen does not explicitly show "the negotiation is aborted if authentication fails."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-37) *"[if] the . . . credential is not valid, then the transaction is aborted. . . ."*would have been selected in accordance with "the negotiation is aborted if authentication fails. . . ." because such validation would have provided an *"electronic object integrity . . . check. . . ."*(See Rosen col. 6, ll. 11-12).

As per claim 45, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 37.

Rosen (col. 16, ll. 19-20) shows elements that suggest a "secret key, verifies the signature of the issuer on the END. . . ."

Rosen (FIG. 1; FIG. 2; FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; col. 40, ll. 14-29; and col. 18, ll. 17-37) shows elements that suggest "the buyer's document carrier after decrypting the message using its secret key, verifies the signature of the issuer on the END, and informs the issuer in the event that authentication fails."

Rosen does not explicitly show "after decrypting the message using its secret key, verifies the signature of the issuer on the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-35) *"[validate] issuer certificate and check issuer signature. . . . Verify . . . identifiers. . . . Validate each sender certificate and check each sender signature. Verify . . . receiver identifier. . . . "* would have been selected in accordance with "after decrypting the message using its secret key, verifies the signature of the issuer on the END. . . . . ." because such verification would have provided an *"electronic object integrity . . . check. . . . "* (See Rosen col. 6, ll. 11-12).

As per claim 47, Rosen in view of Chang shows the method according to claim 25.

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "issuing an END on a document-carrier. . . . [preceding] a method of negotiating an END. . . ."

Rosen (col. 23, ll. 9-51; and FIG. 1) shows elements that suggest a "method of negotiating an END [i.e., *"electronic money"*] between seller and a buyer each possessing a tamper-resistant document carrier. . . ."

Rosen (col. 16, ll. 19-20; col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; FIG. 1 and FIG. 2) shows elements that suggest a "carrier having its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data. . . . sending the public encryption key of the buyer's document carrier to the seller's document carrier. . . ."

Rosen does not explicitly show "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ." because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Rosen does not explicitly show "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda (col. 15, ll. 58-63; and col. 16, ll. 39-40) shows elements that suggest "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda proposes serial number modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Pitroda to Rosen, because such modifications would have provided a means of *"storing . . . various [types] of . . . numbers . . . [associated with] financial or personal transactional information."* (See Pitroda col. 2, ll. 55-61).

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers . . . [and] aborting the negotiation if it is not negotiable. . . ."

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "verifying in the seller's document carrier that the END, if it has been stored previously in that document carrier, has a different counter value this time and is therefore negotiable. . . ."

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the counter, sending that encrypted message to the buyer. . . ."

Rosen does not explicitly show " using . . . [the public encryption key] to encrypt the message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham (col. 5, ll. 5-55; and FIG. 8) shows elements that suggest encrypting a "message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham proposes counter modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Abraham to Rosen, because implementation of such modifications would have provided a method of *"access control. . . . individually programmable by the application owner. . . ."* of a digital work. (See Abraham col. 1, ll. 60-65; and col. 2, ll. 1-5).

As per claim 49, Rosen in view of Chang shows the method according to claim 26.

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "issuing an END on a document-carrier. . . . [preceding] a method of negotiating an END. . . ."

Rosen (col. 23, ll. 9-51; and FIG. 1) shows elements that suggest a "method of negotiating an END [i.e., *"electronic money"*] between seller and a buyer each possessing a tamper-resistant document carrier. . . ."

Rosen (col. 16, ll. 19-20; col. 4, ll. 4-37; col. 4 ll. 40-67; col. 5, ll. 1-23; col. 5, ll. 38-61; col. 6, ll. 3-13; FIG. 1 and FIG. 2) shows elements that suggest a "carrier having its own public-secret key pair, in which the END is stored in the seller's document carrier in the form of END data. . . . sending the public encryption key of the buyer's document carrier to the seller's document carrier. . . .

Rosen does not explicitly show "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "the signature generated by the secret signing-key of a document carrier of the issuer of the END. . . ." because such signing would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

Rosen does not explicitly show "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda (col. 15, ll. 58-63; and col. 16, ll. 39-40) shows elements that suggest "the END is stored . . . together with a serial number counter indicative of the number of times that the END has been negotiated. . . ."

Pitroda proposes serial number modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Pitroda to Rosen, because such modifications would have provided a means of *"storing . . . various [types] of . . . numbers . . . [associated with] financial or personal transactional information."* (See Pitroda col. 2, ll. 55-61).

Rosen (FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "establishing mutual recognition between the seller and buyer using a predetermined protocol between the respective document carriers . . . [and] aborting the negotiation if it is not negotiable. . . ."

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100) shows elements that suggest "verifying in the seller's document carrier that the END, if it has been stored previously in that document carrier, has a different counter value this time and is therefore negotiable. . . ."

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using

it to encrypt the message comprising the END together with the counter, sending that encrypted message to the buyer. . . ."

Rosen does not explicitly show " using . . . [the public encryption key] to encrypt the message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham (col. 5, ll. 5-55; and FIG. 8) shows elements that suggest encrypting a "message comprising the END together with the counter, sending the encrypted message to the buyer . . . and incrementing the counter by one."

Abraham proposes counter modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Abraham to Rosen, because implementation of such modifications would have provided a method of *"access control. . . . individually programmable by the application owner. . . ."* of a digital work. (See Abraham col. 1, ll. 60-65; and col. 2, ll. 1-5).

As per claim 51, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 49.

Rosen (FIG. 1 and FIG. 2) shows elements that suggest "the buyer's document carrier. . . ."

Rosen (col. 16, ll. 19-20) shows elements that suggest a "secret key, verifies that the END is still valid. . . ."

Rosen (col. 6, ll. 37-43) shows elements that suggest "after decrypting the message with its secret key . . . taking its time stamp. . . ."

Rosen (col. 6, ll. 26-32; FIG. 2, els. 58, 84 and 100; and FIG. 7B; col. 2, ll. 61-62; col. 2, line 66; col. 3, ll. 59-60; col. 7, ll. 29-41; col. 13, ll. 35-36; col. 14, ll. 12-35; col. 14, ll. 47-65; col. 15, ll. 3-12; col. 19, ll. 11-40; col. 21, ll. 36-65; col. 22, ll. 5-19; col. 24, ll. 21-60; col. 25, ll. 9-34; col. 27, ll. 15-20; col. 27, ll. 53-61; col. 28, ll. 30-36; col. 29, ll. 52-65; col. 38, ll. 48-67; col. 39, ll. 16-35; col. 39, ll.43-45; and col. 40, ll. 14-29) shows elements that suggest "if . . . [the time stamp] has expired, informs the issuer of this, and aborts the negotiation before incrementing the counter or setting the negotiation status flag."

Rosen does not explicitly show "if . . . [the time stamp] has expired, informs the issuer of this. . . ."; however, it would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 6, ll. 9-12) *"[digital] signatures are well known in the art and are used to detect if a signed electronic object has been altered in anyway since the time it was signed. . . ."* would have been selected in accordance with "if . . . [the time stamp] has expired, informs the issuer of this, and aborts the negotiation before incrementing the counter or setting the negotiation status flag. . . ." because such time stamp validation would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 53, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 37.

Rosen (FIG. 2; FIGs. 30A-E; col. 15, ll. 15-65; col. 16, ll. 1-67; and col. 7, ll. 29-41) shows elements that suggest "recovering the negotiation of an END which has previously broken down, by providing the buyer's document-carrier with the necessary secret key which has been reproduced by the issuer or by a trusted third party."

Rosen does not explicitly show "recovering the negotiation of an END. . . .";

however, it would have been obvious to one of ordinary skill in the art of secure transactions that Rosen (FIG. 2; FIGs. 30A-E; col. 15, ll. 15-65; and col. 16, ll. 1-67) *"recertifying A's certificate. . . ."* would have been selected in accordance with "recovering the negotiation of an END. . . ." because such recertifying validation would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 55, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 37.

Rosen (col. 41, ll. 37-39) shows elements that suggest "an END lost from a primary document-carrier. . . ."

Rosen (col. 13, ll. 5-15; col. 13, ll. 35-60; and col. 20, ll. 31-42) shows elements that suggest "recovering an END lost from a primary document-carrier, by activating a back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier."

Rosen does not explicitly show a "back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen (col. 20, ll. 38-42) *"[the] overall system security pertaining to the money modules may be integrated with that for the trusted agents . . . but is preferably separate to provide for enhanced system security and system flexibility. . . ."* would have been selected in accordance with "a "back-up document-carrier which has previously been provided with back-up data reproduced from the primary document-carrier. . . ." because such back-up capability would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 57, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 53.

Rosen (col. 15, ll. 3-37) shows elements that suggest "inhibiting the recovery until the expiry of the predetermined period of validity of the END."

Rosen does not explicitly show "expiry of the predetermined period of validity of the END."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 15, ll. 3-11) *"[if] the timer expires before the message has been received, then Session Manager A will query Session Manager B to determine if the transaction is still running in B. If B does not reply, then Session Manager will abort the transaction. . . . A similar time-out function exists in the money modules. . . ."* would have been selected in accordance with "expiry of the predetermined period of validity of the

END. . . ." because such a validity transaction would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

As per claim 59, Rosen in view of Chang and Pitroda and further in view of Abraham shows the method according to claim 55.

Rosen (col. 15, ll. 3-37) shows elements that suggest "inhibiting the recovery until the expiry of the predetermined period of validity of the END."

Rosen does not explicitly show "expiry of the predetermined period of validity of the END."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 15, ll. 3-11) *"[if] the timer expires before the message has been received, then Session Manager A will query Session Manager B to determine if the transaction is still running in B. If B does not reply, then Session Manager will abort the transaction. . . . A similar time-out function exists in the money modules. . . ."* would have been selected in accordance with "expiry of the predetermined period of validity of the END. . . ." because such a validity transaction would have provided an *"electronic object integrity . . . check. . . ."* (See Rosen col. 6, ll. 11-12).

8. Independent claim 60 and dependent claim 61 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen in view Halter 5,319,705 (06/07/94) (herein referred to as "Halter").

As per claim 60, Rosen (col. 23, ll. 9-51; FIG. 1; FIG. 2; and FIG. 3) shows elements that suggest a method of negotiating an END sold by a seller to a buyer. . . ."

Rosen does not explicitly show "the buyer splits the End electronically into two or more parts and then negotiates those parts separately to one or more further buyers."

Halter (col. 4, ll. 23-52; and FIG. 2) shows elements that suggest "the buyer splits the End electronically into two or more parts and then negotiates those parts separately to one or more further buyers."

Halter proposes customer distribution modifications that would have applied to the electronic ticket process and system of Rosen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to add the modifications taught by Halter to Rosen, because implementation of such modifications would have provided *"access to encrypted multimedia files. . . ."* to multiple customers of a digital work. (See Halter col. 4, ll. 39-52).

As per claim 61, Rosen in view Halter shows the method of claim 60.

Rosen (col. 4, ll. 51-67; col. 5, ll. 1-23) shows elements that suggest different parts of an END.

Rosen (col. 6, ll. 9-12) shows elements that suggest said "each part is subjected to . . . [a] digital signature of the said buyer's document-carrier which effects the splitting."

Rosen does not explicitly show "each part is subjected to . . . [a] digital signature of the said buyer's document-carrier which effects the splitting."

It would have been obvious to one of ordinary skill in the art of secure transactions that Rosen's (col. 18, ll. 17-35) *"[validate] issuer certificate and check issuer signature. . . . Verify . . . identifiers. . . . Validate each sender certificate and check each sender signature. Verify . . . receiver identifier. . . . "*would have been selected in accordance with "each part is subjected to . . . [a] digital signature of the said buyer's document-carrier which effects the splitting. . . ." because such digital signatures would have provided an *"electronic object integrity . . . check. . . . "*(See Rosen col. 6, ll. 11-12).

RESPONSE TO ARGUMENTS

9. Applicant's arguments (Amendment D, paper#10, filed 02/24/2004) have been fully considered but they are not persuasive, i.e., Applicant's arguments are moot based on new grounds of rejection presented by the Examiner herein.

CONCLUSION

10. Any response to this action should be mailed to:

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Any response to this action may be sent via facsimile to either:

(703)305-7687 (for formal communications EXPEDITED PROCEDURE) or

(703) 305-7687 (for formal communications marked AFTER-FINAL) or

(703) 746-7240 (for informal communications marked PROPOSED or DRAFT).

Hand delivered responses may be brought to:

Seventh Floor Receptionist

Crystal Park V
2451 Crystal Drive
Arlington, Virginia.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John L. Young who may be reached via telephone at (703) 305-3801. The examiner can normally be reached Monday through Friday between 8:30 A.M. and 5:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber, may be reached at (703) 305-8469.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

John L. Young

JOHN LEONARD YOUNG, ESQ.
PRIMARY EXAMINER

Patent Examiner

May 17, 2004